



# CVE-2020-35517

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-35517
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-28 20:15:00 UTC
<b>Updated</b>	2023-02-12 23:41:00 UTC
<b>Description</b>	A flaw was found in qemu. A host privilege escalation issue was found in the virtio-fs shared file system daemon where a pr

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	-	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	-	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link
virtiofsd: avoid /proc/self/fd tempdir · qemu/qemu@ebf1019 · GitHub	MISC	<a href="#">github.com</a>
CVE-2020-35517 QEMU Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
virtio-fs - shared file system for virtual machines	MISC	<a href="#">virtio-fs.git</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.com</a>
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
oss-security - CVE-2020-35517 QEMU: virtiofsd: potential privileged host device access from guest	MISC	<a href="#">www.openwall.com</a>
1915823 – (CVE-2020-35517) CVE-2020-35517 QEMU: virtiofsd: potential privileged host device access from guest	MISC	<a href="#">bugzilla.redhat.com</a>
[PATCH] virtiofsd: prevent opening of special files (CVE-2020-35517)	MISC	<a href="#">lists.gnu.org</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.com</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[198432](#) Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)

[239107](#) Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:0711)

[377152](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2021:0027)

[502353](#) Alpine Linux Security Update for qemu

[710604](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)

[900063](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

[940173](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:0711)

[960678](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:0711)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)